И.Ф. Юшин

Электронные документы как исторический источник

В последние годы особое внимание привлекает проблема, связанная с созданием, распространением, хранением электронных документов (ЭД). Все большее количество производственных и управленческих процессов документируется с помощью компьютерных технологий, реализованных в тех или иных корпоративных информационных системах. Однако качество такого документирования вызывает определенные сомнения. Связано это с тем, что до сих пор не решена задача определения «электронного документа»[1].

Оказывается, что каждая из отраслей знания, связанная с жизненным циклом ЭД, понимает его по-своему и стремится узаконить терминологию, исходя исключительно из своих представлений, часто не учитывающих комплексный характер функционального назначения документа. Поэтому подчас приходится слышать, что ЭД должны рассматриваться только с точки зрения информационных технологий (ИТ), обеспечивающих, прежде всего, скорость передачи и поиска необходимых данных (информации). Некоторые исследователи даже не склонны отличать электронные документы от команд, генерируемых компьютером (например, при связи банкомата с сервером банка)[2].

Заметим, что действительное отличие электронных и аналоговых документов носит принципиальный характер только с одной точки зрения — способе фиксации и воспроизведения информации.

Определение электронного документа в качестве процесса представления информации на экране монитора, процесса передачи данных, формирующих электронный документ и т.п., также как выведение определения электронных документов из терминов электроники и математики (множество реализаций и т.п.[3]) совершенно не учитывают того факта, что «документ» как понятие, применяемое для фиксации правоотношений, не может определять и тем более регулировать сферы, находящиеся вне социальных отношений.

Поэтому, учитывая социальную природу документа в практике делопроизводства, архивного дела используется следующее определение «зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать»[4]. Именно указанное определение и будет ключевым для понимания сущности электронного документа — то есть только та информация, которая целенаправленно зафиксирована, может пониматься и использоваться для изучения фактов, событий, явлений, общественных, правовых, политических и экономических структур.

В этом очерке мы рассматриваем ЭД в первую очередь глазами историка, определяя источниковедческие методики для анализа ЭД, пути и методы извлечения из таких документов необходимой для реконструкции прошлого информации. Заметим, что рассматривая проблему ЭД с точки зрения источниковедения, мы должны позитивно использовать методики и понятийный аппарат, разрабатываемый архиво- и документоведением. Без этого невозможно структурировать ЭД в системе исторических источников.

Определимся, что историческим документом может быть назван любой письменный источник или вещественный остаток прошлого, на котором была зафиксирована письменная информация. Архивным документом определим письменный документ, прошедший процедуру экспертизы ценности и получивший архивные реквизиты.

Ясно, что историк должен уметь работать с любым документом и любым остатком исторического прошлого, на котором отразились результаты человеческой деятельности. Методологию исследования такой профессионал должен не только хорошо знать, но и постоянно развивать – наиболее успешные историки как раз и отличались тем, что их методологические изыскания в области извлечения информации опережали время, и только в редких случаях основывались на больших объемах традиционно обработанной информации.

Опираясь на указанные положения, предлагаем рассмотреть проблему ЭД и их использования современными исследователями социально-гуманитарных процессов прошлого, общественной эволюции, технического и социального прогресса.

* * *

Высокая степень автоматизации и скорость фиксации управленческих и производственных процессов, возможность коллективной работы, быстрота поиска, обработки и применения информации, потенциально возросшая интенсивность получения нового знания — все это обуславливает стремительное проникновение компьютерных систем в органы государственной власти и местного самоуправления, в общественные организации, частный бизнес и приватную жизнь. Тем самым достигается эффективность производства и управленческих процессов, да и самого общественного устройства.

Вместе с тем, самым важным вопросом остается необходимость соблюдения требований целостности и подлинности информации. Общественная эволюция обусловила появление документов для решения этой проблемы. Фиксация информации на каком-либо носителе и придание ей признаков, свидетельствующих о том, что с течением времени она не была фальсифицирована, обеспечило появление не только писцов, архивистов, но дало основания для ускоренного развития права, экономики, а значит и всего общества. Сегодня же развитие социума в свою очередь приводит к тому, что сам документ, приобретая новые качества, лишается самого главного — свидетельств аутентичности и подлинности.

На протяжении первых десятилетий своего существования ЭВМ не обеспечили хранимую в них информацию реквизитами, сравнимыми по важности и однозначности с собственноручной подписью, печатью, формуляром и т.п. В то время проблема традиционно решалась на основе создания защищенных сетей, доступ к которым не могли иметь неавторизованные пользователи. Конечно, и сегодня для обеспечения безопасности информации по-прежнему используются и технические, и организационные (ограничение доступа к технике связи) и технологические (аппаратно-программные модули) методы защиты. Однако возросшая скорость коммуникации и необходимость доступа к большим объемам информации, объединение локальных сетей в глобальные поставили вопрос о принципиально новых способах защиты аутентичности документов.

В условиях, когда существует необходимость одновременной работы с информационными хранилищами Интернета в сочетании с локальными базами данных, проблема конфиденциальности информации и сохранения авторских прав поставила вопрос о новом качестве защитных механизмов. В этих условиях были разработаны технологии, предусматривающие прикрепление аутентифицирующих средств непосредственно к передаваемым ЭД. В этом случае потребовалось, даже не шифруя документ, присовокупить к нему такие подобия реквизитов бумажного документа, которые однозначно удостоверяли бы авторство, подтверждали подлинность и целостность документа, и, в лучшем случае, обеспечивали неоспоримость реквизитов и самого документа.

Заметим, что впервые с необходимостью такого подтверждения столкнулись тогда, когда пришлось аутентифицировать документы, которые не могли быть восприняты человеком без специальных технических средств (аудио-, видеозаписи, внешние носители компьютерной памяти и т.п.).

В течение 60–70-х гг. прошлого века эти проблемы активно решались учеными-управленцами, документоведами и архивистами[5]. Результатом такой работы стало появление «Правил» и ГОСТов, регламентировавших как процесс создания документов на «машинных носителях», так и их описание, хранение, передачу на архивное (постоянное). На каждом этапе здесь было необходимо подтверждать подлинность документа. В нашей стране в середине 1980-х гг. решение было найдено в виде аутентифицирующих признаков, зафиксированных на традиционных аналоговых документах[6].

Ныне, когда речь идет о том, что количество электронных документов растет в геометрической прогрессии, необходимость в прикреплении аналоговых «удостоверителей» для аутентификации электронных вызывает непреодолимые трудности и лишает смысла само их существование. В современных условиях усложнения компьютерной техники и технологии невозможно оперировать многими старыми правилами, стандартами и методиками. Кроме того, за последние три десятка лет значительно ускорился процесс смены программного обеспечения (ПО), а данные (информация) для сохранения подвергались не только переформатированию, но и миграции с различных компьютерных платформ на наиболее распространенные.

Конечно, в этих условиях желательна некая стандартизация аппаратного и программного обеспечения, однако вал электронных

документов уже грозит захлестнуть общество, которое на сегодняшний день не может с полным основанием считать распространяемые ЭД аутентичными (полными и целостными)[7]. В этой связи отметим, что само это явление отнюдь не зависит от того, регулируется ли оно законодательно. Скорее наоборот, именно внедрение компьютерных технологий требует законодательного регулирования этого процесса в сфере документирования. Спрос на доказательную аутентификацию данных, сформированный в последние 10–15 лет привел к появлению программных средств — в первую очередь разного рода ключей аутентификации и электронной цифровой подписи — которые стали активно использоваться в частно-правовой сфере.

* * *

Попробуем сформулировать, что же такое современный ЭД?

Позволим себе рассматривать электронные документы в качестве подмножества документов, существующих исключительно в электронно-цифровой форме[8]. Для историка же важно осознать, что историческим документом может быть любое письменное свидетельство прошлой реальности, отразившее деятельность человека и сохранившее аутентифицирующие признаки такой деятельности. Исторический документ – часть комплекса исторических источников.

Для того, чтобы квалифицированно работать с источником следует детально рассмотреть вопрос о том, что же аутентифицируют реквизиты ЭД?

Так, данные информационных лент Интернета можно идентифицировать как документы, полученные из архивов информационных агентств, однако только на тот момент, когда эти данные были извлечены[9]. Следует понимать, что информационные агентства не ручаются за то, что в их архивах будет храниться первичная информация, а на мониторе и жестком диске пользователя окажутся в итоге изображения и файлы идентичные источнику информации.

Сами аутентифицирующие признаки могут иметь разную степень достоверности и дополнять (проникать в) электронный документ на разных этапах его жизненного цикла. В зависимости от полноты указанных реквизитов, аутентифицирующих документ со времени его создания до архивного хранения (использования), можно выделить электронные документы в узком и широком смыслах.

Электронные документы в *узком смысле* этого слова — это документы, удовлетворяющие требованиям документоведческих и архи-

воведческих стандартов, т.е. документы, аутентифицирующие их автора/создателя и неприкосновенность их состава и структуры *с момента создания*. Поэтому обращение с такими документами столь же традиционно, как и поход в архив, где Вам предложат обстоятельные сведения для внешней критики исторического источника, которые послужат хорошей базой для дальнейшего доказательства достоверности документа и реконструкции действительных исторических фактов.

Разработки таких методик ведутся с двух сторон — историками, изучающими ретроспективу, и архивистами/делопроизводителями, работающими на перспективу. При этом историки занимаются в основном поиском методик доказательства достоверности, архивисты — обеспечением аутентичности, сохраняемой с течением времени[10], а делопроизводители — тщательной фиксацией важных деловых процессов. Именно архивы обеспечивали ранее аутентичность документов, оставляя проблему доказательства достоверности историкам и другим пользователям. Сохранение неприкосновенности документа предоставляло базу для его внутренней критики. Поэтому в случае с электронными документами именно архивы оказываются самыми заинтересованными сторонами — без решения проблемы доказательства аутентичности само их будущее ставится под вопрос.

Рассмотрим, какие же основания существуют ныне для признания документа аутентичным? По действующему ныне закону «Об ЭЦП» документ, подписанный с помощью сертифицированного средства ЭЦП, может полностью отвечать таким требованиям[11]. Для этого создается не только определенный математический аппарат, реализованный в развивающихся программных средствах, нормативная среда, но и объемная организационная структура, представленная системами сертификации, создания, распространения и удостоверения сертификатов подписи и, надеемся, системой долговременного хранения и подтверждения сертификатов подписей.

Согласно закону для подписания документа и проверки его аутентичности используются «закрытый» и «открытый» ключи подписи, представляющие собой последовательность символов определенной длины, создаваемые в процессе выдачи сертификата ключа подписи в удостоверяющем центре. Этот последний сертифицируется органом государственной власти, осуществляющим регулирование в данной области. Обладатель закрытого ключа осуществляет с его помощью

своеобразное «подписание» электронных документов этим «аналогом собственноручной подписи». При этом для того, чтобы распознать достоверность этой подписи и, таким образом, аутентичность подписанного документа, необходимо обладать «открытым ключом подписи», который можно получить в том же удостоверяющем центре.

Смысл такого алгоритма в том, что используемое программное средство, генерирующее аналог собственноручной подписи, позволяет проверить достоверность подписи, даже не зная «закрытого» ключа. Такого рода алгоритмы закреплены специальными ГОСТами, на основе которых происходит сертификация программных средств на соответствие. Иные алгоритмы (реализованные в «симметричных» (DES, IDEA[12]) или «асимметричных» (RSA, DSS[13]) методах шифрования) не соответствуют отечественным ГОСТам и поэтому не могут быть использованы в органах государственной власти и местного самоуправления. Их использование в частных структурах не запрещено, но следует иметь ввиду, что никто кроме авторов (да и, пожалуй, спецслужб) не может сказать, есть ли «лазейка» в используемых здесь функциях, позволяющая разгадать алгоритм и раскрыть «закрытые» ключи.

ГОСТ, определяющий длину закрытого ключа подписи, предполагается обновлять не реже, чем раз в пять лет, поскольку быстро растет вычислительная мощность, совершенствуется математический аппарат, что увеличивает возможность «компрометации» ключей подписи[14].

С другой стороны, защищенные ЭЦП документы именно по этой причине не могут приниматься на долговременное хранение. Не существует и возможности пролонгированного хранения средств аутентификации — по сути это то же ПО, которое устаревает очень быстро. Однако его использование ко всему прочему влечет за собой необходимость работать со сложными и дорогими лицензиями ФАПСИ[15]. И если мы хотим хранить документы в электронном виде, то должны подразумевать необходимость постоянно производить их переформатирование и даже миграцию с одной компьютерной платформы на другую в процессе которых подпись может быть утрачена. Кроме того, она «устаревает» с окончанием срока ее действия, равно как и устаревает само средство ЭЦП.

Тем не менее, различные виды ЭЦП и ее более простые аналоги, такие как «ключи аутентификации» (КА) достаточно широко распространены в частноправовой сфере, хотя практически не действуют

в публично-правовой. Их доступность и высокий спрос на средства аутентификации приводят к широкому распространению несертифицированных средств (импортных, созданных не на основе алгоритмов ГОСТа). Однако в столь чувствительной сфере документационного обеспечения государство не может полагаться на импортируемые средства. Ведь ограничения на длину ключа, введенные в США на экспортируемые криптографические средства, существуют для того, чтобы у правительства Соединенных Штатов существовала возможность в короткий срок раскрыть любое сообщение, «разгадав» любой закрытый ключ подписи. Поэтому опираться придется на отечественные разработки, которые существуют, для которых частично создана нормативная и организационная среда[16].

Но ЭЦП не панацея для архивов и историков. Скорее всего, ЭЦП будет применяться к документам с ограниченными сроками хранения, и ограничения эти будут определены только одним поколением программных средств (в соответствии с проектом закона «Об электронной торговле» не допускается копирование ЭД, кроме как создание бумажных копий). Поэтому, следует признать, что, скорее всего, ЭД, принимаемые в архивы, не будут защищены никакими (ни сертифицированными, ни иными) электронными подписями. Поскольку нельзя хранить ЭЦП долговременно, придется или «снимать» подпись, или «перезакрывать» ее постоянно обновляющейся активной ЭЦП архива — для текущего подтверждения аутентичности хранимого документа. При этом пока невозможно представить, каким образом сохранять аппаратно и программно зависимые комплексы генерирования и проверки устаревших ЭЦП.

Вторая большая проблема состоит в том, что в архив будут поступать — а точнее, архив обязан брать — не только сертифицированные продукты, но и иные, в том числе и не содержащие средств аутентификации документы.

Очевидно, в *широком смысле* слова электронным документом может быть признан любой документ с любыми признаками идентификации. Однако в этом случае следует четко представлять, что же аутентифицируют указанные реквизиты.

Именно в этой сфере аппарат исторического источниковедения еще недостаточно отработан, поскольку у нас практически нет никаких оснований для реконструкции фактов, свидетельства о которых дошли до нас через череду никем и ничем не контролируемых и даже не описанных процессов миграции и переформатирования докумен-

тов. Здесь на каждой стадии мы получаем новый документ с идентифицирующими признаками последней миграции — вот поэтому доказательство аутентичности/достоверности становится малореальными, и, в лучшем случае, вы идентифицируете некую виртуальную реальность, электронное пространство, не существовавшее в действительности, представляющее собой не только продукт технологий, но и идеологий.

С этих позиций рассматривает ЭД и К. Тибодо, отметивший, что при каждом прохождении административных (организационных) границ документ должен приобретать необходимые аутентифицирующие признаки, подтверждающие его целостность и достоверность[17]. Тогда и только тогда мы сможем проследить его историю с момента создания до конечного пользователя. Таким конечным пользователем и будет являться читатель архива ЭД.

К электронным документам в широком смысле этого слова можно отнести Интернет-«документы», данные информационных агентств, разного рода мультимедиа-продукты, исследовательские базы данных, банки данных и информационные ресурсы фискальных, пенсионных, социальных и других государственных органов и т.д., в том числе и документацию частных предприятий, верифицируемую несертифицированными средствами.

Нельзя не остановиться на таком пласте современных компьютерных систем, в массовом порядке генерирующих документы, как системы управления документооборотом, обычно ныне интегрируемые в корпоративные информационные системы. Очевидно, их анализ должен будет проводиться с учетом того факта, что на государственное хранение пока не могут быть приняты в электронном виде документы из этих систем — они не соответствуют ни устаревшим ГОСТам, ни новому закону «Об ЭЦП». Работа исследователя с данными таких систем должна опираться на его высокую квалификацию в области информатики, делопроизводства и документоведения, историческую (источниковедческую) грамотность и профессиональное «чутье». Никаких общих методик работы пока не предложено, и изучение документов следует отложить до того, как будут исследована вся документация о системе, в том числе и та, что лежала в основе формирования технического задания на ее проектирование.

Заметим, что обычно системный администратор, обладающий правами высшего уровня может безбоязненно вмешиваться в функционирование таких систем и не оставляя следов изменять храня-

щиеся документы. Система фиксации доступа к документам в этом случае должна иметь своим итогом четкую последовательность документов, которые бы ежедневно распечатывались или записывались на неперезаписываемый носитель и удостоверялись бы уполномоченным лицом[18].

Многим из указанных там требований удовлетворяют специализированные системы для хранения информации в архиве.

Существующие системы «электронных архивов», часто предполагают создание единого технологического цикла от приема до использования документов, в том числе и с помощью удаленного доступа. В эту цепочку может быть включено и оцифрование документов. Здесь уместно указать на необходимые требования, которые должны быть выдвинуты к системам, внедряемым в архивах. Прежде всего, она должна быть «самодокументирована» — то есть фиксировать все действия, производимые с документами. С другой стороны, система хранения должна предусматривать использование таких носителей, которые позволят максимально затруднить фальсификацию записей. Так, записывая информацию в единый файл, система не дает возможности уничтожить или фальсифицировать документы без полной его перезаписи. Последнее затруднительно произвести бесследно и реализовать беспрепятственно[19].

Индексирование и описание документов в таких системах предусмотрено, однако в случае с электронными документами резоннее предполагать составление описания, аккумулирующего в процессе обращения все основные характеристики жизненного цикла. В этом будет дополнительные основания для внутренней критики источника и для реконструкции исторического прошлого.

Такой подход позволяет по-новому взглянуть и на многочисленные современные публикации, посвященные рассмотрению электронных документов в качестве исторических источников и предлагающие многочисленные методики работы с ЭД как в узком, так и в широком смысле. Конкретные разработки, посвященные методикам исследования новых информационных массивов, чередуются ныне со статьями, разрабатывающими или намечающими целые направления источниковедческих исследований[20]. Различающиеся по глубине источниковедческого исследования, они предлагают разнообразные методики работы с ЭД:

— внутренняя критика источника. Исследование ПО, носителей, универсальных средств – ОС, шрифтов;

— анализ информационных систем (ИС), информационных хранилищ, оценка систем с точки зрения сохранения полноты, целостности и подлинности документов.

Сегодня перед источниковедением становится задача огромной важности, сравнимая с эпохой зарождения самой этой научной дисциплины. Выработка методологии исторической науки нового виртуального мира — достойная задача кибериисториков третьего тысячелетия. Добраться до исторического факта через внешнюю и внутреннюю критику источника (порой обуславливающую само появление такого документа) становится все труднее. Источниковеды должны понять, что для их дисциплины наступает новая эра. Эра очень подвижных источников, которые не имеют характеристик прежнего документа. Источниковедение должно выработать новые методики работы с ними. Историки оказались в среде больших информационных массивов, которые в основном не только не «освящены» хранением в стенах архивов, никак археографически не описаны, подвержены изменениям (!) и даже могут исчезнуть[21].

Примечания

[1] По-прежнему в системах производственной, технической и управленческой документации ИТ используются главным образом для подготовки официальных документов. Под документированием по-прежнему понимается запись информации по установленным правилам — т.е. удостоверение информации с помощью установленных процедур, выраженных в установленных законодательством реквизитах документа (собственноручная подпись, печать, унифицированная форма документа и т.п.). Любое рассмотрение документов вовне организации потребует именно таких реквизитов, исключение составляет разве что межбанковский обмен платежами. Однако отметим, что самым значительным разногласием остается не только различие в понимании удостоверяющих реквизитов, но и попытки дать определение электронного документа используя понятийный аппарат ИТ, находящийся вне документоведения и архивоведения.

[2] *Гадасин В.А.* Общая оценка законодательной базы в сфере электронного документооборота. http: //www.vniipvti.ru/stat/st2.htm, п.8. Полностью фраза звучит следующим образом: «Разрешение банка на получение клиентом денег из банкомата дается машиной, не человеком, которая создает, запрашивает, получает, обрабатывает, передает, хранит более десятка ЭлД (электронных документов! — *И.Ю.*). Лишь время от времени компьютер формирует без участия человека сводный документ, который и анализиру-

ется мыслящим субъектом. Компьютеру безразличен смысл документа, для него «информация» — всего лишь маркированное особым образом подмножество двоичных символов. Электронная информация лишается содержания, смысла, знания, присущего ей в человеческой среде».

[3] *Гадасин В.А., Конявский В.А.* На пороге революции по Гуттенбергу-Федорову. «Connect! Мир связи». № 1. 2002 г. С. 10–1; № 2. 2002 г. С. 18–20 или http://www.vniipvti.ru/stat/st13.htm. Определение, данное соавторами: «Электронный документ — это множество неразличимых по критерию упорядоченности (эквивалентных) реализаций. Количество реализаций (мощность множества) не лимитируется, более того, может меняться в зависимости от места, времени и способа отображения ЭлД (электронных документов — *И.Ю.*)». Оба автора — доктора технических наук, сотрудники НИИ проблем вычислительной техники и информатизации (ВНИИ ПВТИ).

[4] Федеральный закон «Об информации, информатизации и защите информации» от 20 февраля 1995 г., ГОСТ 6.30–97. «Унифицированные системы документации. Унифицированная система организационно-распорядительной документации. Требования к оформлению документов». ГОСТ Р 51141–98. «Делопроизводство и архивное дело. Термины и определения».

[5] *Тихонов В.И., Юшин И.Ф.* Становление и развитие архивов машиночитаемых данных в 1960–1980-е гг. // Отечественные архивы. № 6. М. 1999. С. 42–43. *Тихонов В.И., Юшин И.Ф.* Электронные документы и архивы: опыт и перспективы. // Круг идей: историческая информатика на пороге XXI века. М., 1999. С. 236–238.

[6] ГОСТ 6.10.4–84. «Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения». «Положение о порядке отбора, приема на архивное хранение и выдачи потребителям документов, созданных средствами вычислительной техники». М. 1983. «Перечень научно-технической документации, подлежащей приему в государственные архивы СССР и методические рекомендации по экспертизе ценности научно-технической документации». М, 1987.

[7] Единого стандарта платформ (да и форматов) не существует, хотя в последнее время появилась отсутствовавшая ранее возможность миграции данных с одной платформы на другую, предоставляемая самими разработчиками аппаратно-программного обеспечения. Ранее для того, чтобы провести миграцию данных с магнитных лент, например, БЭСМ-6 в файлы IBM-совместимых микрокомпьютеров требовалось самостоятельно создавать программное обеспечение.

[8] ФЗ «Об электронной цифровой подписи» дает следующее определение: «электронный документ — документ, в котором информация представлена в электронно-цифровом виде». Согласно ГОСТ 6.30–97 «Унифицированные системы документации. Унифицированная система организаци-

онно-распорядительной документации. Требования к оформлению документов», документом является зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать. В.И.Тихонов считает, что исходя из указанного определения реквизиты ЭД могут быть представлены как в электронно-цифровой, так и в бумажной форме (удостоверяющий лист по ГОСТ 6.10.4–84).

[9] Понятно, что подписка на информационные ленты обуславливает получение доступа к почтовой службе агентств (пароли, коды аутентификации и т.п.), при котором обе стороны были бы уверены в однозначной идентификации друг друга. Только таким образом отсекаются попытки неправомерного доступа и обеспечивается невозможность последующего отказа агентств от исходящих документов. Этих реквизитов может быть достаточно для обеих сторон договора. В случае спора арбитражный суд может рассмотреть претензии партнеров, поскольку такое решение принято еще в 1993 г. Высшим арбитражным судом.

[10] Тихонов В.И. Когда наступит время компьютерной палеографии? // Круг идей: историческая информатика в информационном обществе. М., 2001. С. 343–370.

[11] Федеральный закон «Об электронной цифровой подписи» от 09.02.2002 г.

[12] К симметричным методам относят и определяемые ГОСТ 28147. «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования».

[13] К асимметричным относят регламентируемый ГОСТ Р 34.10. «Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма» и ГОСТ Р 34.11. «Функция хэширования». В симметричных методах один и тот же ключ используется и для шифровки, и для расшифровки сообщений. В асимметричных методах применяются два ключа — открытый и закрытый. При реализации ЭЦП закрытый ключ применяется для подписания документа, открытый — для проверки подписи.

[14] Для тех, кто хочет почитать подробнее о криптографических алгоритмах, рекомендуем книгу *Б.Анина* «Защита компьютерной информации». СПб., 2000. Ныне длина ключа определена в 1024 бит.

[15] В России единственным органом, уполномоченным проводить сертификацию, является Федеральное агентство правительственной связи и информации при Президенте Российской Федерации (ФАПСИ). Орган этот подходит к вопросам сертификации очень тщательно. Совсем мало разработок иностранных фирм смогли получить сертификат ФАПСИ.

[16] Федеральная целевая программа «Электронная Россия». http://www.e-russia.ru/program/. Оценку этой программы с точки зрения архивиста можно посмотреть в *Тихонов В.И., Юшин И.Ф.* Будут ли в «электронной» России электронные архивы // Отечественные архивы № 5. 2002.

[17] См. *Duranti L.* The impact of digital technology on archival science // Archival Science, № 1, 2001, pp. 39–55; *Thibodeau K.* Preservation and migration of

electronic records: the state of issue. Выступление на XIV международном конгрессе архивов. Севилья, сентябрь 2000 г.

[18] Требования такого рода изложены в новом стандарте на управление документацией (Record management) ISO 15489.

[19] Интегральная Автоматизированная Информационная Система (ИАИС) Московского городского объединения архивов. Эта система разработана под Oracle. Существуют и иные системы, такие, например, как «Саперион», предлагаемый для распространения корпорацией «Электронный архив».

[20] См., например: *Давлетшина Н.В.* Массивы материалов СМИ как исторический источник по российской истории новейшего времени // Круг идей: историческая информатика в информационном обществе. М., 2001. С. 290–319. *Сменцарев Г.В.* Определении и использовании гуманитарных знаний в сети Интернет // Там же. С. 320–331. *Владимиров В.Н.* Интернет для историка: и все-таки новая парадигма. // Там же. С. 279–289. *Злобин Е.В.* Internet как исторический источник для изучения военных проблем новейшей российской истории // Круг идей: историческая информатика на пороге XXI века. М. 1999. С. 263–293. См. также материалы дискуссии по статье Д.В. Гутнова «Опасности глобальной информатизации гуманитарной науки (заметки заинтересованного наблюдателя)», опубликованные в Бюллетене Ассоциации «История и компьютер» № 26/27, ноябрь 2000 г. М., 2000 С. 128–171.

[21] *Юшин И.Ф.* Источниковедение и архивоведение в цифровую эпоху: очень недоверчивые сестры // Бюллетень Ассоциации «История и компьютер» № 30. 2002 г.